0318045-SNY

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-087078

(43)Date of publication of application : 31.03.1995

(51)Int.Cl. H04L 9/00
G06F 13/00
G09C 1/00
H04L 9/06
H04L 9/10
H04L 9/12
H04L 9/14

(21)Application number : 05-180917

(22)Date of filing : 25.06.1993

(71)Applicant : ROORERU INTELLIGENT SYST:KK

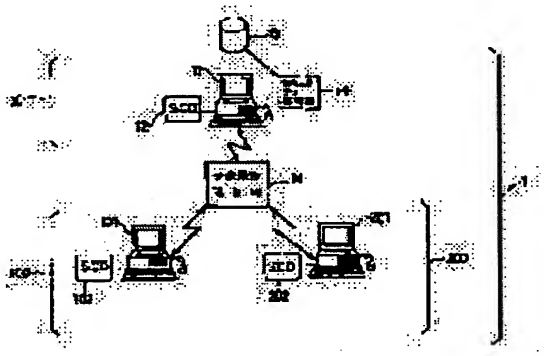
(72)Inventor : TORIKAI MASAMICHI
FUJII MIKIO

(54) INFORMATION TRANSMISSION SYSTEM

(57)Abstract:

PURPOSE: To attain the transmission reception of information in a complete security state by connecting a ciphering device to a terminal device, applying ciphering processing to a specific user password with a ciphering algorithm, creating a terminal identification key able to specify the terminal device, confirming the validity of the terminal device based on the terminal identification key and sending the information.

CONSTITUTION: A security server means 10 is connected to lots of file server means 100 and file receiver means 200 by utilizing a public communication network N. The security server means 10 uses a central device 11 and a ciphering device 12 connecting to the central device 11 to attain transmission reception of ciphered information between terminal devices 101, 201 of each file server means 100 and each file receiver means 200. Furthermore, the file server means 100 includes terminals devices 101... and each ciphered device 102 connecting to each terminal device 101 and registers each terminals device 101 and attains transmission/reception if ciphered information.



LEGAL STATUS

[Date of request for examination] 17.04.2000

[Date of sending the examiner's decision of rejection] 19.08.2003

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－87078

(43)公開日　平成７年(1995)３月31日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/00				
Ｇ０６Ｆ　13/00	３５１　Ｚ	7368－5Ｂ		
Ｇ０９Ｃ　1/00		9364－5Ｌ		
Ｈ０４Ｌ　9/06				
			Ｈ０４Ｌ　9/00	

審査請求　未請求　請求項の数６　ＦＤ　（全９頁）　最終頁に続く

(21)出願番号　特願平5－180917

(22)出願日　平成５年(1993)６月25日

(71)出願人　591234204
株式会社ローレルインテリジェントシステムズ
神奈川県横浜市港区あざみ野１丁目14番５

(72)発明者　烏　飼　将　迪
神奈川県横浜市港区あざみ野１丁目14番５　株式会社ローレルインテリジェントシステムズ内

(72)発明者　藤　井　幹　雄
神奈川県横浜市港区あざみ野１丁目14番５　株式会社ローレルインテリジェントシステムズ内

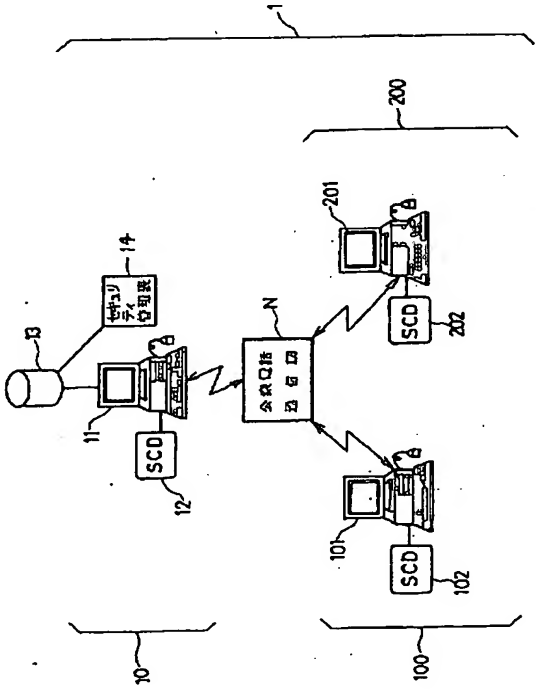
(74)代理人　弁理士　岡田　和宮

(54)【発明の名称】　情報伝送システム

(57)【要約】

【目的】　平文情報を秘密化された暗号化手段により暗号化し、特定の情報授受手段間においてのみ情報の伝達を可能とした伝送システムの提供。

【構成】　予め登録された正当な端末デバイス間で情報を伝送しうる情報伝送システムであって、前記の端末デバイスには、暗号デバイスを接続しており、個有のユーザ暗証と暗号アルゴリズムにより前記の端末デバイスを特定しうる端末識別キーを創成し、当該端末識別キーにより端末デバイスの正当性を確認した後、情報を伝送するものであって、情報提供側の端末デバイスでは、暗号化処理キーを創成し、当該暗号化処理キーを利用して暗号化実行キーを生成して機密ファイルを暗号化ファイルに変換して発信し、又情報受領側では、復号化処理キーを利用して暗号化ファイルを解読するようにしたもの。



【特許請求の範囲】
【請求項１】　予め登録された正当な端末デバイス間で情報を伝送しうる情報伝送システムであって、前記の端末デバイスには、暗号デバイスを接続しており、個有のユーザ暗証を暗号アルゴリズムにより暗号化処理して前記の端末デバイスを特定しうる端末識別キーを創成し、当該端末識別キーにより端末デバイスの正当性を確認した後、情報を伝送するように構成した情報伝送システム。
【請求項２】　端末デバイスを備えたファイルサーバ手段と、ファイルレシーバ手段との間に同様の端末デバイスを備えたセキュリティサーバ手段を介在させて、情報を授受しうるようにした請求項１記載の情報伝送システム。
【請求項３】　前記セキュリティサーバ手段においては、前記ファイルサーバ手段と、ファイルレシーバ手段とに乱数キーを送信しうる手段と、前記ファイルサーバ手段とファイルレシーバ手段とから返信された端末識別暗号キーを前記乱数キーにより復号化し、更に認証キーにより暗号化処理することにより前記ファイルサーバ手段と、ファイルレシーバ手段の暗号化端末識別キーを登録しうる手段を備えており、前記ファイルサーバ手段と、ファイルレシーバ手段においては、各端末識別キーの創成と、各端末識別キーを前記乱数キーによって暗号化して端末識別暗号キーを創成して、これを前記セキュリティサーバ手段に返信しうる手段とを備えた請求項１又は２記載の情報伝送システム。
【請求項４】　前記セキュリティサーバ手段にあっては、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して照合キーを生成すると共に、前記ファイルサーバ手段から返信された端末識別キーによって乱数キーを暗号化した確認キーと、当該照合キーとを照合させて、前記ファイルサーバ手段の端末デバイスの正当性を認証しうる手段を具備してなる請求項１乃至３記載の情報伝送システム。
【請求項５】　前記セキュリティサーバ手段にあっては、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して暗号化処理キーを求めると共に、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して復号化処理キーを生成する手段を備えており、当該暗号化処理キーをファイルサーバ手段に送信し、ファイルサーバ手段においては、その端末識別キーにより前記暗号化処理キーを復号化して暗号化実行キーを生成し、当該暗号化実行キーにより機密ファイルを暗号化して、前記セキュリティサーバ手段に返信しうる手段を含んでいる請求項１乃至４記載の情報伝送システム。
【請求項６】　前記セキュリティサーバ手段にあっては、前記暗号化ファイルと共に、前記復号化処理キーをファイルレシーバ手段に送信する手段を含んでおり、ファイルレシーバ手段にあっては、その端末識別キーにより復号化処理キーを復号化して復号化実行キーを求め、当該復号化実行キーにより、暗号化ファイルを復号化処理して平文情報を受領しうる手段を備えている請求項１乃至５記載の情報伝送システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】この発明は、公衆電話回線などの通信網を利用した情報伝送技術において、登録された特定の端末デバイス間においてのみ情報の伝送を保障しうる情報伝送システムに関するものである。
【０００２】
【従来の技術】従来、トレードシークレットなどの貴重な機密情報を安全に保管し、又は、伝送するために平文情報を暗号化処理し、パソコンなどの端末デバイスを公衆電話回線によって接続して授受する技術は広く活用されており、この際、情報伝送の当事者の確認は、通常例えば、ＩＤコードやパスワードなどによっているところである。
【０００３】しかしながら、悪意の第三者が、不当に前記のＩＤコードもしくはパスワードを知得すれば任意の端末デバイスから容易に当該機密情報にアクセスし、これを詐取することは必ずしも不可能ではなく、実際上、当該機密情報にアクセスして来た端末デバイス自体の正当性を確認することは、別途電話通信による逆探知手法によるとしても、相当の所要時間を費やすこととなり、この端末デバイスそのものの正当性を確認することは殆ど不可能であるため、機密情報の伝送処理には、不安がつきまとうものであった。
【０００４】このような不安を解消するための具体的な改善例としては、例えば、特開昭６３－１５５９３０号公報（公知例）の発明が知られている。
【０００５】この公知例のデータ暗号化通信方式は、公衆データ網を利用して、プロトコル変換手段により変換されたデータを、暗号化キーを付加情報としたパケットとして伝送し、保有する復号化手段の特定キーに基づいてデータの復号化を図るようになしたものである。
【０００６】
【発明が解決しようとする課題】前記の公知例のものにあっても情報を暗号化して、これを伝送しうるものであるが、その目的とするところは、暗号化手段を保有しないデバイス間で公衆データ網を利用して暗号化データを伝送するものであるから、不特定の第三者によるデータ通信デバイスを用いた暗号化情報へのアクセスはフリーとなり、重要な情報の漏洩を完全に未然防止する点での不安が残るものであり、機密情報の伝送に携わるユーザ側からは、暗号化情報が特定の正当な端末デバイス間においてのみ授受されることが保障されうるように、その

保有する端末デバイスの登録，確認を図って常時安心して機密情報の保管・伝送が可能な情報伝送手法の提供が切望されており、この発明の目的とするところは、かかるユーザニーズに応えうる、以下の如き優れたシステムを提供することである。

【０００７】(1) 機密情報を暗号化処理して安全に伝送可能である。

【０００８】(2) 情報伝送に関与できる端末デバイスを予め登録し、利用される端末デバイスの正当性を確認した後に機密情報を伝送させるため、ＩＤコードやパスワードなどを知得しただけでは機密情報にアクセスすることは出来ない。

【０００９】(3) 端末デバイスの登録・確認に際して、活用される暗号化端末識別キーを創成する端末識別キーを乱数キーによって復号化し、さらに認証キーによってこれを暗号化処理したものであるため、機密情報の発信側と受信側の双方において、前記暗号化端末識別キーの守秘性が確保され、機密情報の漏洩を未然防止しうるものである。

【００１０】

【課題を解決するための手段】前記の目的を達成するための、この発明の構成について見れば、次の通りである。

【００１１】(1) 予め登録された正当な端末デバイス間で情報を伝送しうる情報伝送システムであって、前記の端末デバイスには、暗号デバイスを接続しており、個有のユーザ暗証を暗号アルゴリズムにより暗号化処理して前記の端末デバイスを特定しうる端末識別キーを創成し、当該端末識別キーにより端末デバイスの正当性を確認した後、情報を伝送するように構成した情報伝送システム。

【００１２】(2) 端末デバイスを備えたファイルサーバ手段と、ファイルレシーバ手段との間に同様の端末デバイスを備えたセキュリティサーバ手段を介在させて、情報を授受しうるようにした前記(1) 記載の情報伝送システム。

【００１３】(3) 前記セキュリティサーバ手段においては、前記ファイルサーバ手段と、ファイルレシーバ手段とに乱数キーを送信しうる手段と、前記ファイルサーバ手段とファイルレシーバ手段とから返信された端末識別暗号キーを前記乱数キーにより復号化し、更に認証キーにより暗号化処理することにより前記ファイルサーバ手段と、ファイルレシーバ手段の暗号化端末識別キーを登録しうる手段を備えており、前記ファイルサーバ手段と、ファイルレシーバ手段においては、各端末識別キーの創成と、各端末識別キーを前記乱数キーによって暗号化して端末識別暗号キーを創成して、これを前記セキュリティサーバ手段に返信しうる手段とを備えた前記(1) 又は(2) 記載の情報伝送システム。

【００１４】(4) 前記セキュリティサーバ手段にあっては、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して照合キーを生成すると共に、前記ファイルサーバ手段から返信された端末識別キーによって乱数キーを暗号化した確認キーと、当該照合キーとを照合させて、前記ファイルサーバ手段の端末デバイスの正当性を認証しうる手段を具備してなる前記(1) 乃至(3) 記載の情報伝送システム。

【００１５】(5) 前記セキュリティサーバ手段にあっては、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して暗号処理キーを求めると共に、前記暗号化端末識別キーを認証キーにより復号化して端末識別キーを求め、当該端末識別キーによって乱数キーを暗号化して復号化処理キーを生成する手段を備えており、当該暗号化処理キーをファイルサーバ手段に送信し、ファイルサーバ手段においては、その端末識別キーにより前記暗号化処理キーを復号化して暗号化実行キーを生成し、当該暗号化実行キーにより機密ファイルを暗号化して、前記セキュリティサーバ手段に返信しうる手段を含んでいる前記(1) 乃至(4) 記載の情報伝送システム。

【００１６】(6) 前記セキュリティサーバ手段にあっては、前記暗号化ファイルと共に、前記復号化処理キーをファイルレシーバ手段に送信する手段を含んでおり、ファイルレシーバ手段にあっては、その端末識別キーにより復号化処理キーを復号化して復号化実行キーを求め、当該復号化実行キーにより、暗号化ファイルを復号化処理して平文情報を受領しうる手段を備えている前記(1) 乃至(5) 記載の情報伝送システム。

【００１７】

【作　　用】この発明の構成は以上の通りであって、予め暗号化処理して創成された端末識別キーを利用して暗号化端末識別キーを登録し、情報伝送の際には、利用端末デバイスの正当性を確認した後、暗号化された情報を発信させ、当該情報を受信する側に対しても、正当な登録済みの端末デバイスのみが解読しうる復号化処理キーと共に暗号化情報を提供し、受信する側の正当な端末デバイスにおいて平文情報化するものである。

【００１８】

【実　施　例】次に、この発明の実施例を図面に基づいて説明する。図１には、この実施例の情報伝送システム（１）に関する機能ブロック図が示されており、当該システム（１）を構成するセキュリティサーバ手段（１０）は、公衆電話回線、ＬＡＮあるいはＩＳＤＮ回線などの公衆通信網（Ｎ）を利用して、多数のファイルサーバ手段（１００）ならびにファイルレシーバ手段（２００）に接続されたものである。

【００１９】前記セキュリティサーバ手段（１０）の構成は、中央デバイス（１１）と当該中央デバイス（１１）に暗号デバイス（１２）を結線したものであって、

その機能としては、ファイルサーバ手段（１００）およびファイルレシーバ手段（２００）における各端末デバイス（１０１），（２０１）間の暗号情報の授受を可能とするものであるが、その詳細は後述する。

【００２０】更に、前記ファイルサーバ手段（１００）側においては、端末デバイス（１０１）…と、当該端末デバイス（１０１）…に個別に接続された暗号デバイス（１０２）を含んだ構成とされており、その機能としては、各端末デバイス（１０１）の登録ならびに暗号情報の授受を可能としたものであるが、その詳細についても後述する。

【００２１】又、前記ファイルレシーバ手段（２００）についても、本質的に前記ファイルサーバ手段（１００）の場合と同様に端末デバイス（２０１）…および暗号デバイス（２０２）を含んだ構成とされているものである。

【００２２】従って、必要に応じては、前記ファイルサーバ手段（１００）とファイルレシーバ手段（２００）とが立場を換えて、前記ファイルレシーバ手段（２００）から前記ファイルサーバ手段（１００）に対して暗号情報を提供することが可能であることは容易に理解されるところである。

【００２３】尚、図１において、（１３）はメモリ手段であって、セキュリティ管理表（１４）を含むものである。

【００２４】次に、この実施例のシステム（１）におけるファイルサーバ手段（１００）とファイルレシーバ手段（２００）の端末デバイス（１０１）（２０１）の登録・認証ならびに暗号情報の伝送について、第１の企業をファイルサーバ、又第２の企業をファイルレシーバと仮定し、各々の端末デバイス（１０１）と（２０１）との間の伝送処理のケースを例に挙げて説明すると次の通りである。

【００２５】なお、この出願明細書における情報の暗号化ならびに復号化に関する数式は、式１によるものと定義する。

【００２６】

【数１】

$$KO = D_Z\,[E_Y\,(X)] \quad \cdots\cdots\cdots\cdots \text{式１}$$

【００２７】即ち、この式１の内容は、情報（Ｘ）を暗号キー（Ｙ）により暗号化（エンサイファー）し、更に、暗号キー（Ｚ）により復号化（デサイファー）した結果は、函数出力（ＫＯ）としてとらえることを意味するものである。

【００２８】①　端末デバイスの登録

先ず、情報の伝送に先立って、前記の端末デバイス（１０１）（２０１）の登録を実施しなければならない。

【００２９】その理由は、貴重な機密情報をハンドリングするオペレータについては、パスワードもしくはＩＤコードなどによって確認されるとしても、当該オペレータにより特定の端末デバイスが正当に操作されていることが確認された場合に限って端末デバイスが機能し、情報伝送が可能となるようにすることが情報の漏洩防止のために重要であるが故である。

【００３０】即ち、この点を換言すれば、予め情報伝送処理に関与することが許諾された登録済みの正当な端末デバイス間のみで情報伝送が可能であるから、前記パスワードやＩＤコードなどによるオペレータの確認と併用することにより、情報の機密保持が一層確実に保障されることとなるものである。

【００３１】そこで、以下にこの登録の手順を図２および図３に示すフローチャートをも参照して説明する。

【００３２】(1) 端末識別キー（ＥＳＫ）（ＥＲＫ）の創成

端末識別キー（ＥＳＫ）（ＥＲＫ）とは、前記第１の企業と第２の企業が保持する秘密の独自の「キー」であって、以下に述べるような手順で創成し、これを秘密の状態で保存しうるものである。

【００３３】まず、各端末デバイス（１０１）（２０１）において、０～９の９個の数字と、Ａ～Ｆの６個のアルファベットの合計１６桁の記号群の１６乗（16^{16}）　の乱数から任意の記号群を選定してユーザ個有のユーザ暗証（ＳＫ）（ＲＫ）を決定し、当該端末デバイス（１０１）（２０１）に接続された暗号デバイス（１０２）（２０２）により前記ユーザ暗証（ＳＫ）（ＲＫ）を暗号アルゴリズム（ＡＬ）によって、端末識別キー（ＥＳＫ）（ＥＲＫ）を創設する（ＳＰ１），（ＳＰ２）。

【００３４】尚、前記の暗号アルゴリズムについては、例えば、１９７７年以来、開示済みの米国標準「ＤＥＳ（ＤＡＴＡ　ＥＮＣＲＩＰＴＩＯＮ　ＳＴＡＮＤＡＲＤ）」あるいは、ＮＴＴ社による「ＦＥＡＬ８システム」の如き８バイトを単一のブロックとするブロック暗号化方式のものを利用することが便利であり、これらの暗号アルゴリズム（ＡＬ）については公開されているが、当該アルゴリズムに使用する「キー」であるユーザ暗証（ＳＫ）（ＲＫ）を秘密に保持することにより、当該「キー」を知る者以外の者には解読できない仕組みとなっているため、その守秘性は安全に保障されうるものである。

【００３５】前記の如く、後述の情報伝送に際しての、各端末デバイス（１０１）（２０１）の認証のために重大な判定要素となる端末識別キー（ＥＳＫ）（ＥＲＫ）は、暗号化アルゴリズムによって暗号化処理されているため、第三者によって視認され、もしくは解読されるおそれは皆無であって、秘密保持の安全性は極めて高いものであると言える。

【００３６】(2) 端末デバイス（１０１）（２０１）の登録
次に、図３に示すフローチャートに基づいて、端末デバイス（１０１）（２０１）をセキュリティサーバ手段（１０）に登録する手順について述べると次の通りである。
【００３７】まず、端末デバイス（１０１）（２０１）を操作して中央デバイス（１１）に対して、端末登録の請求を行なう（ＳＰ５）。
【００３８】この登録請求を受理したセキュリティサーバ手段（１０）においては暗号デバイス（１２）から提供された格別の意味を持たない乱数キー（ＲＲ）を、それぞれ前記端末デバイス（１０１）（２０１）に送信する（ＳＰ６）。
【００３９】前記の乱数キー（ＲＲ）を受信した前記端末デバイス（１０１）（２０１）においては、それぞれの暗号デバイス（１０２）（２０２）において、端末識別キー（ＥＳＫ）（ＥＲＫ）を、乱数キー（ＲＲ）によって暗号化して端末識別暗号キー（ＳＳ）（ＲＳ）作成し、これを中央デバイス（１１）へ返信する（ＳＰ７）。この点は、次の式に示す通りである。
【００４０】
【数２】

$$SS = E_{RR}(ESK) \quad \cdots\cdots\cdots\cdots\text{式}2$$

【００４１】
【数３】

$$RS = E_{RR}(ERK) \quad \cdots\cdots\cdots\cdots\text{式}3$$

【００４２】次に、セキュリティサーバ手段（１０）においては、各端末デバイス（１０１）（２０１）の暗号化端末識別キー（ＳＺ）（ＲＺ）の登録を行なうこととなるが、その内容は、暗号デバイス（１２）において端末識別暗号キー（ＳＳ）（ＲＳ）を乱数キー（ＲＲ）によって復号化し、更にこれを認証キー（ＣＫ）により暗号化して各端末デバイス（１０１）（２０１）の暗号化端末識別キー（ＳＺ）（ＲＺ）を生成するものであって、その式は次の通り、
【００４３】
【数４】

$$SZ = E_{CK}[D_{RR}(SS)] \quad \cdots\cdots\cdots\text{式}4$$

【００４４】
【数５】

$$RZ = E_{CK}[D_{RR}(RS)] \quad \cdots\cdots\cdots\text{式}5$$

【００４５】となり、これを、中央デバイス（１１）に登録し、メモリ手段（１３）にあるセキュリティ管理表（１４）に格納・保管することにより、端末デバイス（１０１）（２０１）の登録が完了する（ＳＰ８）。
【００４６】② 暗号情報の授受
次に、端末デバイス（１０１）から平文情報の機密ファイル（ＦＬ）を端末デバイス（２０１）へ伝送する場合について見れば、図４に示す通りである。
【００４７】(1) 端末デバイス（１０１）の確認
【００４８】まず、端末デバイス（１０１）から中央デバイス（１１）に対して機密ファイル（ＦＬ）の伝送請求がなされる（ＳＰ９）。
【００４９】セキュリティサーバ手段（１０）においては、この請求が真正な端末デバイス（１０１）からなされたものであることを確認するために、乱数キー（ＲＲ）を端末デバイス（１０１）へ送信すると共に、照合キー（ＭＫ）を内製する（ＳＰ１０）。
【００５０】この照合キー（ＭＫ）の内製の手順については、端末デバイス（１０１）の暗号化端末識別キー（ＳＺ）を認証キー（ＣＫ）によって復号化し、求められた端末識別キー（ＥＳＫ）によって乱数キー（ＲＲ）を暗号化して生成するものであって、その式は次の通りとなる。
【００５１】
【数６】

$$ESK = D_{CK}(SZ) \quad \cdots\cdots\cdots\cdots\text{式}6$$

【００５２】
【数７】

$$MK = E_{ESK}(RR) \quad \cdots\cdots\cdots\cdots\text{式}7$$

【００５３】一方、前記の乱数キー（ＲＲ）を受信した端末デバイス（１０１）においては、暗号デバイス（１０２）によって当該乱数キー（ＲＲ）を端末識別キー（ＥＳＫ）で暗号化処理して確認キー（ＳＡ）を作成し、セキュリティサーバ手段（１０）へ返信する（ＳＰ１１）ものであり、その式は次の通りである。

【００５４】

【数８】

$$SA = E_{ESK}\ (RR) \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{式}8$$

【００５５】その後、この確認キー（ＳＡ）を前記照合キー（ＭＫ）と照合し（ＳＰ１２）、その結果が一致すれば、ファイル伝送請求が第１の企業の端末デバイス（１０１）からなされたものであることが確認され、ファイル伝送が許可されることとなるが（ＳＰ１３）、この照合の結果が不一致であれば、例えば、図示しない表示，警報手段などにより報知させうるものである（ＳＰ１４）。

【００５６】なお、この照合作業に併せて、第１の企業の端末デバイス（１０１）のオペレータに関して、例えば、ＩＤコードやパスワードなどを照合させ、その合致を確認することにより、尚一層の情報の漏洩防止に寄与できるものであることは前記の如く言うまでもないことである。

【００５７】(2) 機密ファイルの伝送

次に、機密ファイル（ＦＬ）の伝送請求を受理したセキュリティサーバ手段（１０）においては、端末デバイス（１０１）特有の暗号化処理キー（ＡＡＫ）を生成し、これを端末デバイス（１０１）へ送信することとなるが、その操作は、暗号化端末識別キー（ＳＺ）を認証キー（ＣＫ）で復号化して端末識別キー（ＥＳＫ）を生成することとなるが、その式は次の通りとなる。

【００５８】

【数９】

$$ESK = D_{CK}\ (SZ) \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{式}9$$

【００５９】次で、この端末識別キー（ＥＳＫ）により乱数キー（ＲＲ）を暗号化して、暗号化処理キー（ＡＡＫ）を得るものであるが、この式は次の通りである。

【００６０】

【数１０】

$$AAK = E_{ESK}\ (RR) \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{式}10$$

【００６１】又、更に、中央デバイス（１１）においては、機密ファイル（ＦＬ）の伝送先である端末デバイス（２０１）における暗号デバイス（２０２）の復号化処理キー（ＢＢＫ）をも作成するが、その操作は、その暗号化端末識別キー（ＲＺ）を認証キー（ＣＫ）で復号化して得られた端末識別キー（ＥＲＫ）によって、乱数キー（ＲＲ）を暗号化して復号化処理キー（ＢＢＫ）を生成するものであって、次の式に示す通りである。

【００６２】

【数１１】

$$ERK = D_{CK}\ (RZ) \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{式}11$$

【００６３】

【数１２】

$$BBK = E_{ERK}\ (RR) \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{式}12$$

【００６４】この復号化処理キー（ＢＢＫ）はメモリ手段（１３）に保存するとともに、前記の暗号化処理キー（ＡＡＫ）のみを端末デバイス（１０１）へ送信する（ＳＰ１５）。

【００６５】この暗号化処理キー（ＡＡＫ）を受理した端末デバイス（１０１）においては、暗号デバイス（１０３）により暗号化処理キー（ＡＡＫ）を端末識別キー（ＥＳＫ）により復号化することにより暗号化実行キー（ＡＡＺ）を生成する（ＳＰ１６）ものであり、次式の通りである。

【００６６】

【数１３】

$$AAZ = D_{ESK}\ (AAK) \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{式}13$$

【００６７】又、この暗号化実行キー（ＡＡＺ）により機密ファイル（ＦＬ）を暗号化して、暗号化ファイル（ＡＦＬ）を作成する（ＳＰ１６）ものであり、次式の通りである。

【００６８】

【数１４】

$$AFL = E_{AAZ}\ (FL) \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{式}14$$

【００６９】次に、端末デバイス（１０１）により、この暗号化ファイル（ＡＦＬ）をセキュリティサーバ手段（１０）に送信する。

【００７０】この暗号化ファイル（ＡＦＬ）を受信したセキュリティサーバ手段（１０）においては、当該暗号化ファイル（ＡＦＬ）と共に前記の復号化処理キー（ＢＢＫ）についても端末デバイス（２０１）へ送信する（ＳＰ１７）。

【００７１】(3) ファイルの受信と復号化

【００７２】次に、これらの送信を受けた端末デバイス（２０１）側の暗号デバイス（２０２）においては、復号化処理キー（ＢＢＫ）を、端末識別キー（ＥＲＫ）によって復号化して、復号化実行キー（ＢＢＺ）を得るが、これは次式の通りである（ＳＰ１８）。

【００７３】

【数１５】

$$BB = D_{ERK}\ (BBK) \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{式}15$$

【００７４】次で、この復号化実行キー（ＢＢＺ）により暗号化ファイル（ＡＦＬ）を復号化して、機密ファイル（ＦＬ）を平文情報に復帰させて受領しうるものであって、次の式に示す通りである（ＳＰ１８）。

【００７５】

$$FL=D_{BBZ}\ (AFL)\quad\cdots\cdots\cdots\cdots\cdots\text{式}16$$

【００７６】なお、この実施例においては、第１の企業と第２の企業に設置された特定の端末デバイス間における情報の伝送処理について記述したが、これ以外に、例えば、本社と支社、あるいはホームバンキングの如く金融機関と端末手段を設置した一般家庭の間においても、同様に機密情報の授受をなしうるものであることは言うまでもないことである。

【００７７】又、前記の実施例においては、その技術内容の理解を助成するためにファイルサーバ手段（１００）と、ファイルレシーバ手段（２００）とを単一対状に図示して説明したが、ファイルサーバ手段（１００）とファイルレシーバ手段（２００）とは、適宜複数個併設し、それらの間で情報の授受をなしうるように構成しうることは詳しく説明するまでもなく当然のことであり、ファイルサーバ手段（１００）のみならず、ファイルレシーバ手段（２００）のいずれにも、暗号デバイス（１０２）（２０２）が接続されているから、機密情報をセキュリティサーバ手段（１０）を仲介することなく、ファイルサーバ手段（１００）からファイルレシーバ手段（２００）へ直接に機密情報を伝送するように操作することも可能なことであることは、重ねて説明するまでもないことである。

【００７８】

【発明の効果】以上の通り、この発明によれば、平文情報を暗号化処理して機密の状態で安全に伝送されるばかりでなく、情報の授受に関係する端末デバイスが予め登録された端末識別キーを具備していることを認証することによって、正当な端末デバイスであることが確認された後に、暗号化された情報の発信を実行するものであり、加えて、情報を受信する側の端末デバイスについても、同様に正当な登録を受けた端末デバイスに限って情報を受領し、その解読のための復号化処理キーの提供をうけて、当該暗号化情報を平文情報に解読できるものであり、完璧に機密状態で情報の授受が可能である。

【００７９】又、暗号化端末識別キーを創成する端末識別キーがユーザ暗証と暗号アルゴリズムによって創成するものであるから、端末識別キーの秘密保存が安全に保障されて機密情報の漏洩の防止を一層確実にさせうるものである。

【図面の簡単な説明】

【図１】この発明の実施例を示す機能ブロック図。

【図２】図１における端末識別キー創成のフローチャート。

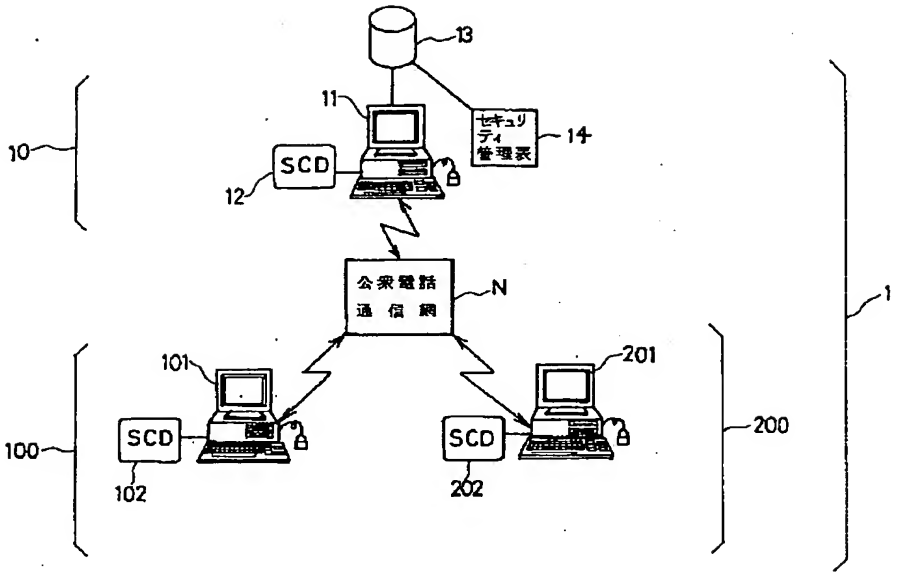
【図３】図１における端末登録のフローチャート。

【図４】図１における情報伝送のフローチャート。

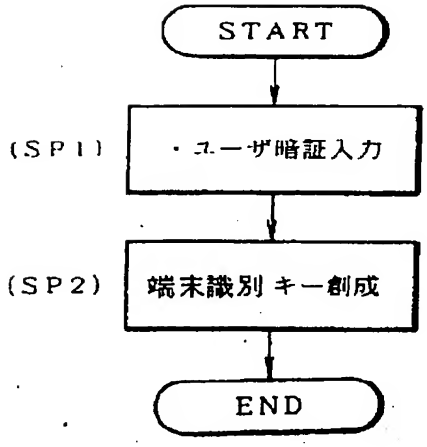
【符号の説明】

１	情報伝送システム
１０	セキュリティサーバ手段
１１	中央デバイス
１０１，２０１	端末デバイス
１２，１０２，２０２	暗号デバイス
１３	メモリ手段
１００	ファイルサーバ手段
２００	ファイルレシーバ手段
ＡＬ	暗号アルゴリズム
ＳＫ，ＲＫ	ユーザ暗証
ＳＺ，ＲＺ	暗号化端末識別キー
ＳＳ，ＲＳ	端末識別暗号キー
ＥＳＫ，ＥＲＫ	端末識別キー
ＳＡ，ＲＡ	確認キー
ＲＲ	乱数キー
ＦＬ	機密ファイル
ＡＦＬ	暗号化ファイル
ＭＫ	照合キー
ＣＫ	認証キー
ＡＡＫ	暗号化処理キー
ＡＡＺ	暗号化実行キー
ＢＢＫ	復号化処理キー
ＢＢＺ	復号化実行キー

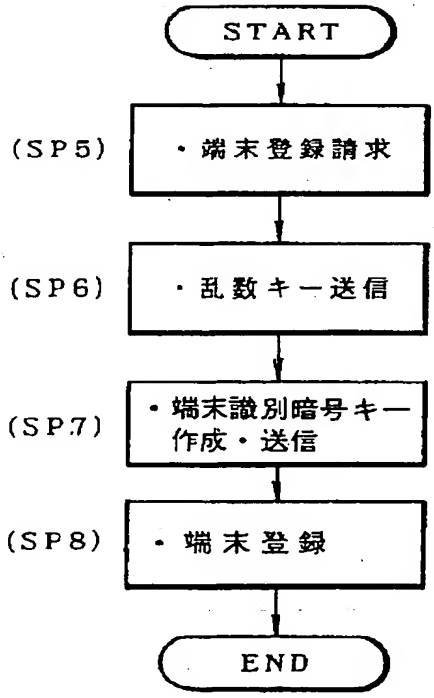
【図１】



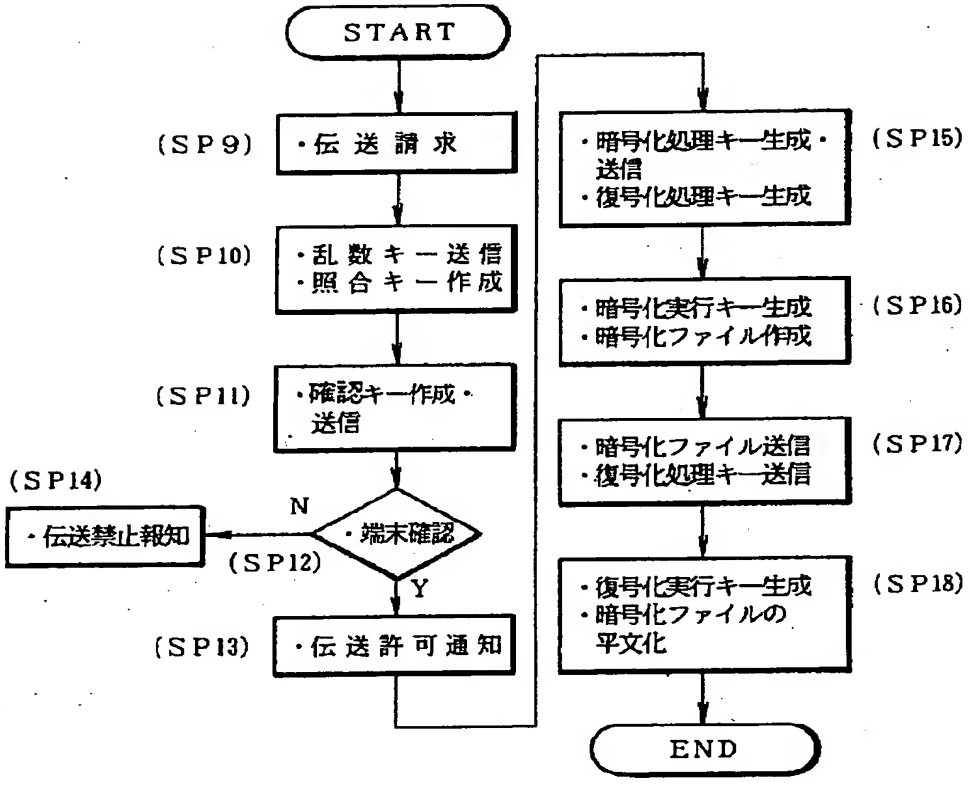
【図２】



【図３】



【図４】



フロントページの続き

(51) Int. Cl.⁶		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｈ０４Ｌ	9/10				
	9/12				
	9/14				